WEST

Generate Collection Print

L2: Entry 1 of 2 File: JPAB Jul 18, 2000

PUB-NO: JP02000200311A
DOCUMENT-IDENTIFIER: JP 2000200311 A
TITLE: ELECTRONIC BID SYSTEM

PUBN-DATE: July 18, 2000

INVENTOR-INFORMATION:

NAME	COUNTRY
SAKO, KAZUE	

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NEC CORP	

APPL-NO: JP10374833
APPL-DATE: December 28, 1998

INT-CL (IPC): G06 F 19/00; G09 C 1/00

ABSTRACT:

PROBLEM TO BE SOLVED: To provide an efficient electronic bid system for guaranteeing the propriety of a highest bid price while concealing bidding prices other than the highest bid price.

SOLUTION: A cryptographic parameter depending on the bidding price is supplied to the part of an enciphering function in a bidder subsystem 100, and the bidding price is enciphered based on this cryptographic parameter. Concerning deciphering in a bid disclosure subsystem 200, the enciphered data are deciphered successively from deciphering parameters successively corresponding to the maximum or minimum successful bidding price, and the data deciphered successfully are discriminated as the bidding price corresponding to the parameter and become the highest bid price. The deciphering parameters corresponding to the bidding prices of ranking lower than the highest bid price are not disclosed, so that non-successful bidding price information is concealed.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－200311
（P2000－200311A）
(43)公開日　平成12年７月18日(2000.7.18)

(51)Int.Cl'	識別記号	FI		テーマコード'(参考)
G06F 19/00		G06F 15/28	B	5B049
G09C 1/00	630	G09C 1/00	630Z	5J104
	660		660Z	9A001

審査請求 有　請求項の数4 OL （全６頁）

(21)出願番号　特願平10－374833

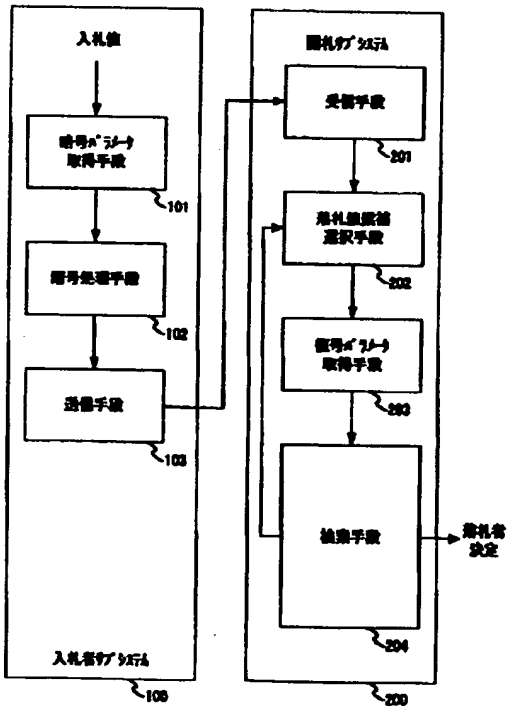
(22)出願日　平成10年12月28日(1998.12.28)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　佐古　和恵
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100105511
弁理士　鈴木　康夫　（外１名）

Ｆターム(参考)　5B049 BB36 CC31 EE05 GG10
5J104 AA01 AA16 DA04 EA19 PA00
PA10
9A001 EE03 JJ64

(54)【発明の名称】　電子入札システム

(57)【要約】
【課題】　落札値以外の入札値を秘匿しながら、落札値の正当性を保証する効率のよい電子入札システムを提供する。
【解決手段】　入札者サブシステム１００における暗号化機能の部分に、入札値に依存した暗号パラメータを供給し、この暗号パラメータに依存して入札値暗号化する。開札サブシステム２００における復号は、落札可能な入札値のうち最大あるいは最小のものから順最大の入札値に対応する復号パラメータから順に暗号データを復号し、無事に復号できたものはそのパラメータに対応する入札値であると判定され落札値となる。落札値以下の順位の入札値に関する復号パラメータは公表しないことにより、落札されなかった入札値情報は秘匿される。



1

【特許請求の範囲】

【請求項1】　複数の入札者が呈示する入札値のうち最大あるいは最小の値を落札値とする電子入札システムにおいて、

入札者サブシステムが入札可能な範囲から選んだ入札値を入力として、該入札値に依存した暗号パラメータを取得する暗号パラメータ取得手段と、前記暗号パラメータ取得手段で入手した暗号パラメータを用いる暗号処理手段と、前記暗号処理手段で暗号化した暗号文を開札サブシステムに送信する送信手段を有する入札者サブシステムと、

前記暗号化された入札値を締切日まで受け付ける受信手段と、落札可能な入札値のうち最大あるいは最小のものから順次落札値候補を選択する選択手段と、前記選択手段が選択した落札値候補に対応する復号パラメータを取得する復号パラメータ取得手段と、前記復号パラメータを用いて前記受信手段が受け付けた暗号化された入札値を復号することにより前記選択手段が選択した落札値候補と同じ入札値が前記受信手段が受け付けた暗号化された入札値の中に存在するか否かを検索する検索手段を有する開札サブシステムからなることを特徴とする電子入札システム。

【請求項2】　前記入札サブシステムの暗号処理手段は、前記暗号パラメータ取得手段で入手した暗号パラメータを用いて既定値を暗号化し、前記開札サブシステムの検索手段は、前記復号パラメータ取得手段で取得した復号パラメータに基づき前記受信手段が受信した暗号入札値に対して順次復号処理をする復号処理手段と、復号処理結果が前記既定値になった場合にその暗号入札値が前記選択手段で選択した落札値候補と同一であると判定する判定手段を有していることを特徴とする請求項1記載の電子入札システム。

【請求項3】　前記入札者サブシステムの暗号処理手段は、前記入札値に対応した公開鍵で既定値を暗号化する処理を含み、前記開札サブシステムの復号処理手段は、該入札値に対応した公開鍵に対応する秘密鍵で復号する処理を含むことを特徴とする請求項1または2記載の電子入札システム。

【請求項4】　前記開札サブシステムは、最大値を落札値とする場合には、前記入札された暗号入札値の全てと前記落札値より大きい入札可能値に対応する復号パラメータあるいは復号結果を、また、最小値を落札値とする場合には、前記入札された暗号入札値の全てと前記落札値より小さい入札可能値に対応する復号パラメータあるいは復号結果を公表する公表手段を有していることを特徴とする請求項1～3のいずれかに記載の電子入札システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子入札システムに関し、特に入札値の暗号化方法および落札値決定方法に関する。

2

【0002】

【従来の技術】このような電子入札システムは、例えば特開平2-118876号公報に見られるように、一般的に開札まで入札値情報を秘匿する必要があるため、暗号化技術が取り入れられている。暗号化された入札値情報は、開札時に一斉に復号され、そのうちの最大あるいは最小の入札値が落札値として決定される。そして、全ての入札値を公開することによって、落札値が正当に決定されたこと、すなわち入札値のうちで最大あるいは最小の値であったことを誰でも確認することができるようになっている。

【0003】近年、プライバシー保護の目的で、落札に至らなかった入札値を公開しないことが要求されている。この要請に応えるために、例えば、IEEE Workshop on Dependable and Real-Time E-Commerce Systemにて発表されたKikuchi,Harkavy,Tyger著の論文Multi-round Anonymous Auction Protocolsに開示されている手法がある。この先行技術文献に開示された手法を図3に示す。

【0004】この手法においては、入札者は、入札値に対応するデータ列を生成し、それぞれのデータを分割して暗号化する。開札者は、全入札者から送付された暗号列データを受信して統合したのちに復号し、落札値を決定する。この手法では、入札者単位で暗号列データを復号しないので、各入札者の入札値を秘匿できるとともに、全入札者の暗号列データを統合することにより、最大の値を入札した人の識別情報を抽出することができる。

【0005】以下、識別情報が抽出できる原理について説明する。識別情報ＩＤｉを持つ入札者は、入札値に対応するデータ列を以下の通りに作成する。すなわち入札可能な範囲が（ａ，ｂ）であり、入札値がａ＋ｖ（＜ｂ）であったとすると、まず、ｖ＋１個のＩＤ＿ｉを列挙する。次にｂ－（ａ＋ｖ）個の０を列挙する。このようにして（ｂ－ａ＋１）個の要素からなるデータ列を生成する。

【0006】このように生成された全入札者からのデータ列を統合すると、データ列の各要素を要素ごとに加算したデータ列が出力される。このデータ列において、最初に０が現れた要素がｔ番目だとすると、最大の入札値（落札値）はａ＋ｔ－１であり、落札者はｔ－１番目の要素の値の示す識別情報を持つ人である。

【0007】

【発明が解決しようとする課題】ところが、この従来技術では、入札可能な範囲の長さに比例したデータ列を作成し、さらにそれを分割して暗号化することにより、入札データが入札可能な値の範囲に比例して長くなるという問題がある。さらには、落札値を入札した人が複数い

た場合、ｔ－１番目の要素の復号結果が該当入札値の入札者のＩＤ情報の和になっているので、誰が該当者なのか、該当者が何名いるのか判別できないという問題もある。

【０００８】本発明の主な目的は、入札データを少なくすることができるとともに、落札値を入札した人が複数いた場合であっても誰が該当者か判別することができ、さらに落札者以外の入札値の入札情報を秘匿できる電子入札システムを提供することにある。

【０００９】

【課題を解決するための手段】本発明による電子入札システムは、入札者サブシステムにおける暗号化機能の部分に、入札値に依存した暗号パラメータを供給し、また、開札サブシステムにおいて落札値を決定するために、落札値候補選択機能と、候補値に依存した復号パラメータによる復号機能を設けたことを特徴としている。

【００１０】この暗号パラメータ及び復号パラメータを導入することにより、入札値と落札値候補が同一であるか否かのみを判定できるという作用を実現する。従って、落札値候補を入札可能な最大値あるいは最小値からひとつずつ推移させながら、落札値候補と同一の入札値があるかどうかを判定すれば、最大あるいは最小の入札値及び入札者を決定することが可能であり、さらに、その入札者以外がどのように入札したかは秘匿できるという効果が得られる。

【００１１】

【発明の実施の形態】図１は、本発明の実施の形態を示すブロック図である。本発明の電子入札システムは、入札者サブシステム１００と開札サブシステム２００によって構成される。入札者サブシステム１００は、暗号パラメータ取得手段１０１、暗号処理手段１０２、送信手段１０３を有する。開札サブシステム２００は、受信手段２０１、落札値候補選択手段２０２、復号パラメータ取得手段２０３、及び検索手段２０４を有する。

【００１２】検索手段２０４は、図２に示すように復号処理手段２０５及び判定手段２０６からなり、復号処理手段２０５は、復号パラメータ取得手段２０３で取得した復号パラメータに基づき、受信手段２０１が受信した暗号入札値に対して順次復号処理を行い、判定手段２０６は、復号処理手段２０５による復号処理結果が既定値になった場合に、その暗号入札値が落札値候補選択手段２０２で選択した落札値候補と同一であると判定する。

【００１３】なお、本実施の形態では、説明を簡単にするために、以下、入札された値のうち、最大値を入札した入札サブシステムを落札者であると決定するものとして説明するが、最小値を落札値とする場合であっても同様である。

【００１４】入札者サブシステム１００への入力は、この入札者サブシステムの希望する入札値である。この入札者サブシステム１００に入札された入札値は、暗号パラメータ取得手段１０１に供給される。暗号パラメータ取得手段１０１では、この入札値に依存して暗号処理手段１０２に必要な暗号パラメータを取得し、暗号処理手段１０２に供給する。暗号処理手段１０２は、供給された暗号パラメータに基づいて暗号演算をおこない、暗号入札データを送信手段１０３に供給する。送信手段１０３は、暗号入札データを開札サブシステム２００の受信手段２０１に送信する。

【００１５】開札サブシステム２００の受信手段２０１は、各入札者サブシステム１００から送付された暗号入札データを受信し、開札日に落札値候補選択手段２０２に対して開札の開始を指示する。開札指示を受けた落札値候補選択手段２０２は、まず、落札可能な範囲のうちの最大値を候補値であるとみなして、この候補値を復号パラメータ取得手段２０３に供給する。

【００１６】復号パラメータ取得手段２０３は、この候補値に依存した復号パラメータを取得して、検索手段２０４に供給する。検索手段２０４では、復号処理手段２０５において、供給された復号パラメータを用いて受信した全ての暗号入札データを復号し、判定手段２０６で暗号入札データの中に候補値と同じ入札値のものがあるかどうかを検索する。もしあればその暗号入札データを送信した入札者サブシステムを落札者と決定する。この候補値を入札値として作成された暗号入札データがなければ、検索手段２０４は、該候補値は落札値ではない旨を落札値候補選択手段２０２に出力する。

【００１７】検索手段２０４から落札値ではない旨の信号をうけた落札値候補選択手段２０２は、現在の候補値の次に小さい値を新たに候補値として、復号パラメータ取得手段２０３に供給する。そして、判定手段２０６が落札者を決定するまで、あるいは候補値が入札可能な範囲を下回るまで同様の処理を繰り返す。落札値候補が入札可能な範囲を下回った場合は、落札者なしと判断し、その旨を出力して処理を終了する。

【００１８】以下、本実施の形態の具体例として、暗号化関数にエルガマル暗号を用いた場合について述べる。エルガマル暗号は、当業者にとってよく知られており、また本発明とは直接関係しないので、その詳細な説明は省略する。

【００１９】まず、開札システムは大きな素数ｐと生成元ｇを生成する。また、各入札値ｖに対して、秘密鍵ｘ（ｖ）、公開鍵ｙ（ｖ）と定数Ｍ（ｖ）を決定する。ここで、公開鍵ｙ（ｖ）と秘密鍵ｘ（ｖ）には以下のような関係がある。生成元ｇをｘ（ｖ）乗してｐの剰余をとったものがｙ（ｖ）である。Ｍ（ｖ）は任意の値でよく、例えばＭ（ｖ）としてｖとそのハッシュ値を連結したものでもよいし、またｖに依存せずに定数であってもよい。暗号パラメータとしてＭ（ｖ），ｙ（ｖ）を、復号パラメータとしてｘ（ｖ）を採用する。暗号パラメータは公開し、復号パラメータは開札システム内で厳重に

管理する。

【0020】入札者サブシステム100は、自分の希望する入札値vに対して、暗号パラメータM（v），y（v）を取得し、M（v）を公開鍵y（v）でエルガマル暗号に基づき暗号化する。エルガマル暗号は、確率暗号と呼ばれる種類の暗号に属し、同じM（v）を暗号化しても異なる暗号文になることが知られている。入札者サブシステム100は、この暗号結果を暗号入札データC（v）として開札サブシステム200に送付する。

【0021】開札サブシステム200は、落札値候補v'に対して復号パラメータx（v'）を取得し、この復号パラメータを秘密鍵としてC（v）を復号する。このとき、v=v'であればあきらかに復号結果はM（v）=M（v'）となる。一方、vとv'が等しくない場合、復号結果がM（v'）となることはほとんどない。このようにして、入札値自身を求めずに、落札値候補と等しいかどうかを判定することができる。

【0022】落札値がvと決定された場合、入札された暗号入札値のすべてと、vより大きな入札可能値に対応する復号パラメータx（v）は公表手段により公表される。従って、この公表された復号パラメータを用いて入札された全ての暗号入札値の復号を試すことができるので、vより大きな入札値がなかったことと、誰が落札値を入札したかを誰でも検証することが可能となる。

【0023】一方、落札値より小さな入札可能値に対応する復号パラメータx（v）は公表されないので、落札値より小さな入札値についてはどのようなものがあったかは秘匿できる。さらに、明らかに複数の入札サブシステムが落札値を入札した場合にも、該当入札サブシステムはすべて判明するので、従来方式にあったような落札者が複数存在する場合の問題は生じない。

【0024】他の具体例として、暗号化関数にRSA暗号を用いた場合について述べる。RSA暗号も、当業者にとってよく知られており、また本発明とは直接関係しないので、その詳細な説明は省略する。RSA暗号の場合には、暗号パラメータであるy（v）を表引きしなくても、入札値vから自動的に生成され、また暗号化される既定値M（v）は全入札者に対して既定値でなくてもよい。

【0025】まず、開札システムは大きな素数pとqを生成し、その積をnとする。入札者サブシステムは、自分の希望する入札値vに対して、暗号パラメータM（v），y（v）を下記の様に生成する。すなわち、乱数を生成し、M（v）を、vと、この乱数およびこれらを連結したハッシュ値を連結したものとする。次に、y（v）として、vのハッシュ値に1を連結させ、（p-1）（q-1）と互いに素となる数とする。

【0026】そしてM（v）を公開鍵y（v）で法nのRSA暗号に基づき暗号化する。この場合、各入札者毎に異なる乱数を発生させているので、同じM（v）を暗号化しても異なる暗号文になる。入札者サブシステム100は、この暗号結果を暗号入札データC（v）として開札サブシステム200に送付する。

【0027】開札サブシステム200は、落札値候補v'に対してy（v'）すなわち、そのハッシュ値を計算し、復号パラメータとして、法（p-1）（q-1）においてy（v'）の逆元となるx（v'）を計算する。そして、この復号パラメータを秘密鍵として法nにおいてC（v）を復号する。

【0028】このとき、v=v'であればあきらかに復号結果M（v'）はv'とある乱数による正しいフォーマットになっている。一方、vとv'が等しくない場合には、復号結果がそのようなフォーマットになる可能性はほとんどない。このようにして、入札値自身を求めずに、落札値候補と等しいかどうかを判定することができる。

【0029】落札値がvと決定された場合、入札された暗号入札値のすべてと、vより大きな入札可能値に対応する復号パラメータx（v）により復号処理された各結果が公表手段により公表される。この公表された復号結果を、落札値候補に対応する暗号パラメータy（v'）により暗号化した結果が入札されたそれぞれの暗号入札値に等しいことが確認できるので、vより大きな入札値がなかったことと、誰が落札値を入札したかを誰でも検証することが可能となる。

【0030】一方、落札値より小さな入札可能値に対応する復号結果は公表されないので、落札値より小さな入札値についてはどのようなものがあったかは秘匿できる。さらに、明らかに複数の入札サブシステムが落札値を入札した場合にも、該当入札サブシステムはすべて判明するので、従来方式にあったような落札者が複数存在する場合の問題は生じない。

【0031】また、開札サブシステムに入力される暗号入札値が入札期間外のものを受け付けていないことは、入札期日前に受理した暗号入札値を公開し、開札時に対象となるものはその公開したもののみと限定することで保証することができる。これは本発明とは直接関係しないのでその詳細な説明は省略する。

【0032】さらに、開札サブシステムが不当に暗号入札値を復号しないことは、秘密分散やグループ復号技術などを利用して、復号パラメータを複数のサブシステムで管理あるいは生成することによって保証できる。これも本発明とは直接関係しないのでその詳細な説明は省略する。

【0033】また、入札者が他人の名をかたって入札したり、送付した暗号入札値について後日否認することを防止するために、暗号入札値のデジタル署名を付加することができるが、これも本発明とは直接関係しないのでその詳細な説明は省略する。

【0034】本実施例では、簡単のため入札された値の

うち最大値を入札した入札サブシステムを落札者と決定する場合について説明したが、同様に、最小値を入札した入札サブシステムを落札者とする場合、または、最大値あるいは最小値に近い入札値を入札した複数の入札サブシステムを落札者とする場合にも容易に適用することができる。

【0035】なお、本発明は、上記の各実施例に限定されるものではなく、本発明の技術思想の範囲内において、各実施例を適宜変更して実施可能であることは云うまでもない。

【0036】

【発明の効果】以上説明したように、本願発明によれば、入札者サブシステムが入札値に依存した暗号パラメータにより暗号化し、開札サブシステムが落札値候補に依存した復号パラメータにより復号するという基本構成に基づき、最大あるいは最小の入札値を提出した入札者を落札者と選出でき、かつ落札者以外の入札者の入札データの秘匿を実現した電子入札システムを提供することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態の構成を示すブロック図である。

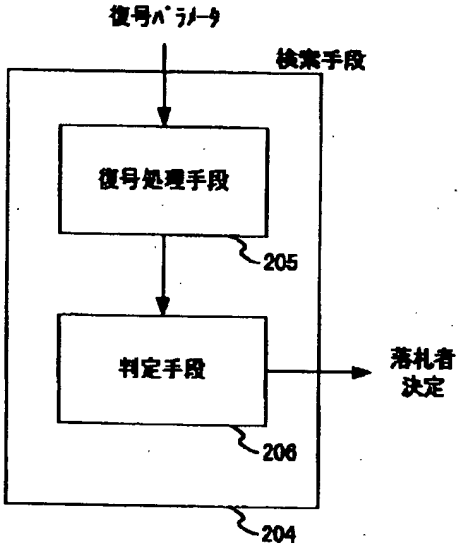
【図2】本発明の検索手段の構成を示すブロック図である。

【図3】従来方式を示すブロック図である。

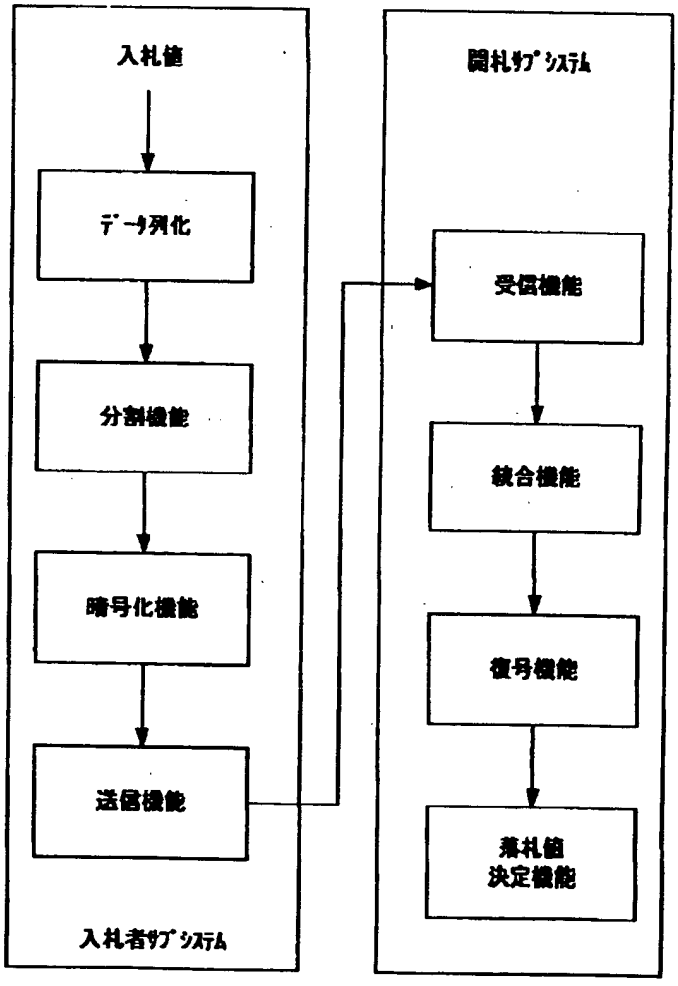
【符号の説明】

100	入札者サブシステム
101	暗号パラメータ取得手段
102	暗号処理手段
103	送信手段
200	開札サブシステム
201	受信手段
202	落札値候補選択手段
203	復号パラメータ取得手段
204	検索手段
205	復号処理手段
206	判定手段

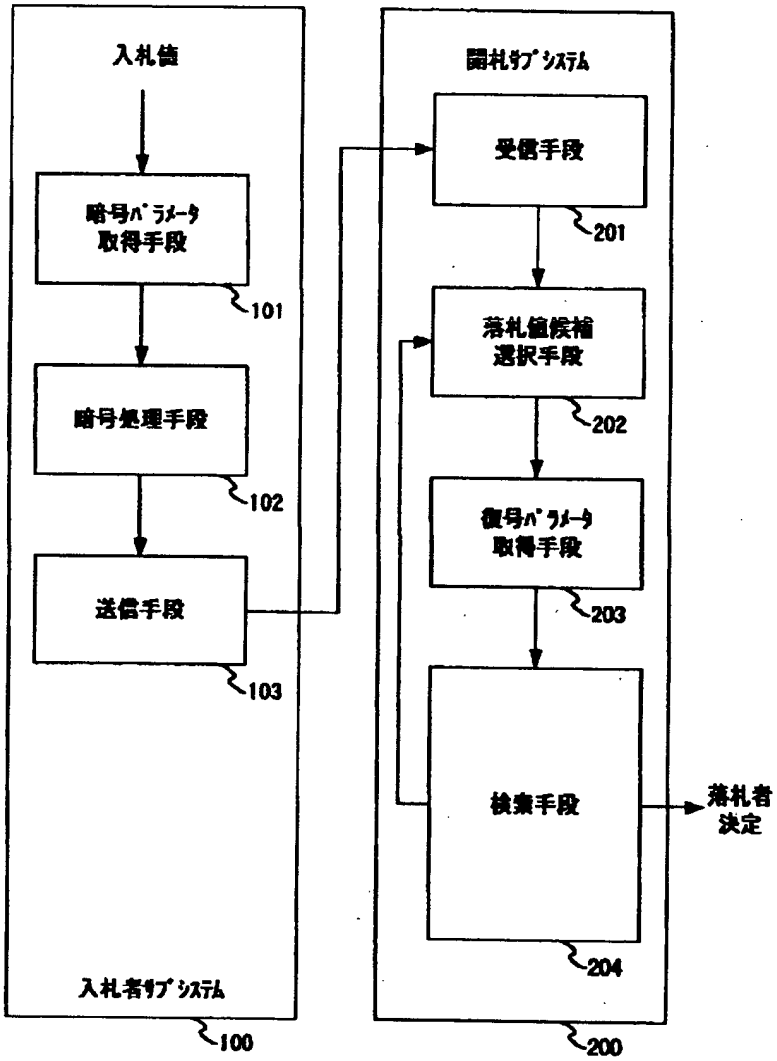
【図2】



【図3】



【図1】


入札者
暗号ﾊﾟﾗﾒｰﾀ
取得手段
101
暗号処理手段
102
送信手段
103
入札者ｻﾌﾞｼｽﾃﾑ
100
開札ｻﾌﾞｼｽﾃﾑ
受信手段
201
落札値候補
選択手段
202
復号ﾊﾟﾗﾒｰﾀ
取得手段
203
検索手段
204
200
落札者
決定